LITE DEPALMA GREENBERG & AFANADOR, LLC
Joseph J. DePalma
Catherine B. Derenze
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

[Additional Attorneys on Signature Page]

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JOSEPH ROLLINS, Individually And On Behalf Of All Others Similarly Situated, *Plaintiff*, v. SAMSUNG ELECTRONICS AMERICA, INC., *Defendant*.	Civil Action No.: _____ **COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff, Joseph Rollins ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Samsung Electronics America, Inc. ("Samsung" or the "Defendant"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based upon, *inter alia*, the investigation of counsel, and review of public documents.

NATURE OF THE ACTION

1. Plaintiff brings this action on behalf of a Nationwide Class and New Jersey Sub-Class (together, the "Classes") against Defendant due to its failure to protect the sensitive and

confidential Personally Identifiable Information ("PII") of millions of customers—including first and last names, dates of birth, postal addresses, precise geolocation data, email addresses, and telephone numbers. Defendant's wrongful disclosure has harmed Plaintiff and the Class, which includes millions of people.

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and is a class action in which there are more than 100 members of the Class, members of the Class (as defined below) are citizens of states different from Defendants, and greater than two-thirds of the members of the Class reside in states other than the states in which Defendant is a citizen.

3. This Court has personal jurisdiction over Defendant because it is headquartered in New Jersey; the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues; and Defendant has intentionally availed itself of this jurisdiction by marketing and selling its products and services in New Jersey.

4. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to Plaintiff's claims occurred in New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

PARTIES

Joseph Rollins

5. Plaintiff Joseph Rollins resides in Browns Mills, New Jersey and is a current Samsung customer. Plaintiff Rollins was notified by Samsung that his PII was compromised in the Samsung data breach.

6. Plaintiff purchased a Samsung Galaxy S10 device that is covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on his Samsung device to monitor personal and confidential health information. Plaintiff also uses his device to view and transact his banking and credit information, make payments, and other day-to-day banking activity.

7. Samsung's warranty, as well as any policies governing the operating systems of the products purchased by Plaintiff, were presented to him on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff prior to his purchase of those products.

8. On or about September 2, 2022, Plaintiff Rollins, and the public, were first notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff Rollins received an e-mail on September 2, 2022 from Samsung notifying Plaintiff that his Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stole from Samsung's servers.

9. As a direct and proximate result of the breach, Plaintiff Rollins has made reasonable efforts to mitigate the impact of the breach, including but not limited to: conducting research concerning this data breach; discussing the breach with his family; reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud; and freezing his credit report. This is valuable time Plaintiff Rollins otherwise could have spent on other activities.

10. Plaintiff Rollins is very concerned about identity theft as well as the consequences of such identity theft and fraud resulting from the data breach. Plaintiff Rollins has received an increased number of phishing emails and spam telephone calls since July 2022, from entities

including pharmacies, solar businesses, and extended warranties. Such emails and calls trick consumers into providing sensitive and valuable personal information to scammers and, in turn, increases the risk of Plaintiff suffering from monetary or identity theft. Plaintiff Rollins has and will spend a significant amount of time responding to the impacts of the data breach. The time spent dealing with the fallout from the data breach is time Plaintiff otherwise would have spent on other activities.

11. Plaintiff Rollins suffered actual injury from having his Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of his Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

12. As a result of the data breach, Plaintiff Rollins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

Defendant

13. Samsung is a New York corporation with its American headquarters and principal place of business located at 85 Challenger Road, Ridgefield, New Jersey 07660-2118.

FACTUAL BACKGROUND

14. Samsung is "recognized globally as an industry leader in technology." It has millions of customers, has an estimated brand value of approximately $45.5 billion, and produces over $200 billion in revenue each year.

15. Samsung manufactures a wide range of consumer and industrial electronic products such as televisions and home appliances (air conditioners, washer and dryers, stoves, refrigerators

and microwave ovens, etc.). Samsung's televisions and home appliances connect to the Internet and require customers to create a "Samsung Account" prior to accessing many of their devices' features.

16. For example, consumers who purchase "smart" televisions typically do so because they want to watch streaming applications, such as Netflix or Hulu, on their televisions rather than on separate devices. Although Samsung advertises that their smart televisions allows owners to have streaming applications at their "fingertips," an owner of a Samsung smart television cannot access those streaming applications without downloading those applications onto their television. But, in order to download those applications, the Samsung smart television owner must create a Samsung Account first.

17. Samsung also produces smart phones, smart watches, and tablets, and offers applications ("apps") for those devices. Samsung's apps include, but are not limited to, Samsung Health, Samsung Cloud, and Samsung Pay. In order to access the features of these devices and apps, Samsung requires customers to create a Samsung Account.

18. A "Samsung Account" is the "gateway to the World of Samsung." A Samsung Account allows customers to not only access certain features that improve the usability of the device, but a Samsung Account also provides device-related benefits that only customers with a Samsung Account can access. Those benefits include, but are not limited to, backing up and syncing data, finding a device when it is lost, device support, coupons and discounts, and order tracking.

Samsung Collects Its Customers' Personally Identifiable Information Because It Is Valuable to Samsung

19. Plaintiff and other proposed Class Members were required, as current and prospective customers of Samsung, to provide Samsung with sensitive Personally Identifiable

Information to purchase or receive Samsung's devices and services.

20. When a customer purchases a Samsung product, creates a Samsung Account, or registers for or uses a Samsung service, the customer may provide Samsung with Personally Identifiable Information such as:

- name;
- email address;
- postal address;
- phone number;
- payment card information (including name, card number, expiration date, and security code);
- date of birth;
- gender
- information stored in or associated with the customer's Samsung Account, including the customer's Samsung Account profile, ID, username, and password;
- username and password for participating third-party devices, apps, features, or services;
- information a customer stores on a Samsung device, such as photos, contacts, text logs, touch interactions, settings, and calendar information;
- recordings of a customer's voice when they use voice commands to control a service or contact Samsung's Customer Service team; and
- location data, including (1) the precise geolocation of a customer's device if they consent to the collection of this data and (2) information about nearby Wi-Fi access points and cell towers that may be transmitted to Samsung when the customer uses certain

Services.

21. Samsung also collects information automatically from its customers concerning their Samsung devices such as their mobile network operator; connections to other devices; app usage information; device settings; web sites visited; search terms used; the apps, services, or features a customer downloads or purchases; and how and when those services are used.

22. Samsung uses the information that it obtains directly from customers and that it collects automatically to:

- "[O]perate, evaluate, and improve our business, including developing new products and services, managing our communications, analyzing our Services and customer base, conducting market research, aggregating and anonymizing data, performing data analytics, and undertaking accounting, auditing, and other internal functions";
- Communicate with its customers; and
- "[P]rovide ads, which may include targeted (or interest-based) ads delivered on your Samsung device or within certain Samsung-branded apps."

23. The Personally Identifiable Information that Samsung collects from its customers is valuable to Samsung. Indeed, Samsung acknowledges this information "plays a key role in elevating what we do for our community" and that it "engage[s] with [Personally Identifiable Information] to inform and enhance everything from your experience to our communication, and to create and innovate radical solutions that help you overcome barriers."

24. Samsung is also aware that its customers value their own Personally Identifiable Information. Samsung acknowledges that its customers "own" their "privacy" and recognizes "the importance [customers] place on the value of [their] privacy".

25. Because Personally Identifiable Information is valuable to Samsung's customers,

Samsung made multiple promises so as to alleviate concerns any customers may have about providing Samsung with this sensitive information.

26. Samsung promised its customers that:

- its devices and services are "designed with privacy and security at top mind";
- it "take[s] data security very seriously";
- it is "committed" to safely handling its customers Personally Identifiable Information;
- it "maintain[s] safeguards designed to protect personal information [Samsung] obtain[s]";
- "security and privacy are at the core of what [Samsung] do[es] and what [it] think[s] about every day";
- it has "industry-leading security";
- it "prioritize[s]" protecting customers' Personally Identifiable Information through certain security measures; and
- it takes "a holistic approach to security to ensure that, at all levels of the device, [it is] protecting users' security and privacy at all times."

27. Moreover, the Federal Trade Commission ("FTC") has established security guidelines and recommendations for businesses that possess their customers' sensitive personally identifiable information to reduce the likelihood of data breaches like Samsung. Among such recommendations are: limiting the sensitive consumer information kept; encrypting sensitive information sent to third parties or stored on computer networks; and identifying and understanding network vulnerabilities.

28. Samsung, thus, had obligations—created by contract, industry standards, common

law, and its representations to its customers like Plaintiff and other Class Members—to keep this Personally Identifiable Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided this Personally Identifiable Information to Samsung with the understanding that Samsung would comply with its own representations as well as its obligations to keep such information confidential and secure from unauthorized disclosures.

29. While Samsung has enriched itself through the collection of a treasure trove of information about Plaintiff and Class Members, and profited off its collection of that information, Samsung failed to employ reasonable, accepted safety measures to secure that valuable information.

The Data Breach

30. On September 2, 2022, the Friday before Labor Day, Samsung released a statement announcing that its "U.S. systems" had been infiltrated "[i]n late July 2022" by "an unauthorized third party" that then stole Personally Identifiable Information that Plaintiff and other putative Class Members had entrusted to Samsung.

31. According to Samsung, the data breach may have affected customers' Personally Identifiable Information such as name, contact and demographic information, date of birth, and product registration information. However, Samsung claims "[t]he information affected for each relevant customer may vary."

32. Samsung claims it did not discover the data breach until "[o]n or around August 4, 2022" after an "ongoing investigation."

33. As of September 2, 2022, Samsung was in the process of notifying affected customers of the data breach.

34. Although Samsung touts that it "always aim[s] to do the right thing by being open

and honest with [its] customers," Samsung did not release a statement to affected customers until almost a month after learning of the data breach.

35. Samsung's statement also was not transparent. The statement did not explain how the data breach occurred, how Samsung discovered the data breach, what Samsung systems were affected, why it took over a month for Samsung to reveal the data breach occurred, the number of Samsung customers that were affected, whether the customers affected were businesses or consumers, what prompted the "ongoing investigation," how long the investigation had been ongoing, or the extent of the Personally Identifiable Information stolen.

36. Chris Clements, Vice President of Solutions Architecture at Cerberus Sentinel, a provider of cybersecurity and compliance services, commented on Samsung's statement announcing the data breach that: "The lack of transparency on the number of individuals impacted as well as the delay in notifying them combined with a late Friday holiday weekend release seem like clear attempts to minimize the incident."

37. Plaintiff and Class Members have been injured by the disclosure of their Personally Identifiable Information in Samsung's data breach.

38. The exposure of Plaintiff's and Class Members' names, dates of birth, contact and demographic information, and product registration information increases their risk exponentially for precision spearphishing attacks, engineered SIM swaps, and the threat of credit and loans being taken out in their names.

39. One of the most concerning aspects of the Samsung Data Breach is the fact that the hackers stole "demographic information" from Samsung. Samsung says is collects demographic information to "help deliver the best experience possible with our products and services" (or to target specific advertising to consumers).

40. Samsung's U.S. privacy policy explains this more explicitly: "Ad networks allow us to target our messaging to users considering demographic data, users' inferred interests, and browsing context. These networks can track users' online activities over time by collecting information through automated means, including through the use of browser cookies, web beacons, pixels, device identifiers, server logs, and other similar technologies."

41. While Samsung has thus far refused to reveal what specific demographic data was stolen, TechCrunch examined Samsung's policies and concluded that this data might include: technical information about your phone or other device, how you use your device, like which apps you have installed and which websites you visit, and how you interact with ads, which are used by advertisers and data brokers to infer information about you. The data can also include your "precise geolocation data," which can be used to identify where you go and who you meet with. Samsung says it collects information about what you watch on its smart TVs, including which channels and programs you have watched.

42. Samsung also says it "may obtain other behavioral and demographic data from trusted third-party data sources," which means Samsung buys data from other companies and combines it with its own stores of customer information to learn more about you, again for targeted advertising. Samsung would not say which companies, such as data brokers, it obtains this data from.

Samsung Has a History of Data Breaches

43. This is not Samsung's first data breach in 2022. Accordingly, Samsung should have been particularly aware of the vulnerability of its security systems.

44. On March 7, 2022, Samsung announced it had suffered a data breach that exposed internal company data, including the source code related to its Galaxy smartphones, algorithms

related to Samsung smartphone biometric authentication, bootloader source code to bypass some of Samsung's operating systems controls, source code for Samsung's activation servers, and full source for technology used for authorizing and authenticating Samsung accounts.

45. The company claimed the data breach did not include the personal information of consumers or employees.

46. The incident came to light after LAPSUS$, a hacking group, leaked 190GB of Samsung's data to four hundred (400) peers.

47. Following the data breach, Samsung promised it would "implement[] measures to prevent further such incidents and will continue to serve our customers without disruption."

48. It is possible that the data breach that Samsung announced on September 2, 2022 could be a continuation of the March 7, 2022 data breach.

49. "Given the difficulty of completely eliminating malware once it has infiltrated a corporate network, especially one as large and complex as Samsung's, the latest incident could well be a continuation of the March hack," said Chad McDonald, CISO of Radiant Logic, an identity and access management vendor.

50. McDonald further stated: "The fact that they sat on this for as long as they did before they did a public disclosure … implies to me they were less concerned about urgency. This makes me feel like this was quite likely just a continuation of [the former breach] they just hadn't discovered yet."

51. Samsung's repeated security failures demonstrate that it failed to honor their duties and promises by not, among other things: maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks; adequately protecting Plaintiff's and the Classes' Personally Identifiable Information; and failing to reasonably limit the sensitive consumer

information kept, in violation of FTC recommendations.

CLASS ACTION ALLEGATIONS

52. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff bring this case as a class action on behalf of a Nationwide Class and a New Jersey Sub-Class, defined as follows:

Nationwide Class

> All persons in the United States whose Personally Identifiable Information was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

New Jersey Sub-Class

> New Jersey Sub-Class: All persons in the State of New Jersey whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

53. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

54. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant owed Plaintiff and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Personally Identifiable Information, and whether it breached that duty;

b. Whether Defendant continues to breach duties to Plaintiff and other Class Members;

c. Whether Defendant's data security systems prior to the data breach met industry

standards;

d. Whether Defendant failed to adequately respond to the data breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay;

e. Whether Plaintiff and other Class Members' Personally Identifiable Information was compromised in the data breach; and

f. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

55. Plaintiff's claims are typical of the Classes' claims. Plaintiff suffered the same injury as Class Members—i.e., Plaintiff's Personally Identifiable Information was compromised in the data breach.

56. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel has interests that are contrary to or that conflict with those of the proposed Classes.

57. Defendant has engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and other Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

58. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the

prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims

59. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST CLAIM FOR RELIEF
Negligence
On behalf of Plaintiff, the Class, and the New Jersey Subclass

60. Plaintiff realleges and incorporates by reference all preceding factual allegations found in paragraphs 1 through 59.

61. To access features of the devices, apps, or services Plaintiff and Class Members purchased, Samsung required Plaintiff and Class Members to submit non-public Personally Identifiable Information to obtain these features.

62. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant both had a duty of care to use reasonable means to secure and safeguard this Personally Identifiable Information, to prevent disclosure of the information, and to guard the information from theft.

63. Defendant's duty included a responsibility to implement a process by which it could

detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

64. Defendant also owed a duty of care to Plaintiff and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that its systems and networks—and the personnel responsible for them— adequately protected Defendant's customers' Personally Identifiable Information.

65. Defendant's duty to use reasonable security measures arose as result of the special relationship that existed between it and its customers. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Classes from a data breach.

66. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

67. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law, statutes, and FTC guidance described above, but also because it is bound by, and has committed to comply with, industry standards for the protection of confidential Personally Identifiable Information.

68. Defendant breached its common law, statutory, and other duties—and thus, was negligent—by failing to use reasonable measures to protect its customers' Personally Identifiable Information, and by failing to provide timely notice of the data breach.

69. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personally Identifiable Information;

b. allowing unauthorized access to Plaintiff's and Class Members' Personally Identifiable Information;

c. failing to recognize in a timely manner that Plaintiff's and Class Members' Personally Identifiable Information had been compromised; and

d. failing to warn Plaintiff and Class Members about the data breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

70. It was foreseeable that Defendant's failure to use reasonable measures to protect Personally Identifiable Information and to provide timely notice of the data breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Classes were reasonably foreseeable.

71. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

72. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
On behalf of Plaintiff, the Class, and the New Jersey Subclass

73. Plaintiff realleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 59.

74. When Plaintiff and Class Members paid money and provided their Personally Identifiable Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

75. Defendant solicited and invited prospective and current customers to provide their Personally Identifiable Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Personally Identifiable Information to Defendant. In entering into such implied contracts, Plaintiff and Class Members assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class Members to pay for adequate and reasonable data security practices.

76. Plaintiff and the Class Members would not have provided and entrusted their Personally Identifiable Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

77. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Defendant.

78. Defendant breached its implied contracts with Plaintiff and the Class Members by failing to safeguard and protect their Personally Identifiable Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data

breach.

79. As a direct and proximate result of Defendant's breaches of its implied contracts, Plaintiff and the Class Members sustained actual losses and damages as described herein.

THIRD CLAIM FOR RELIEF
Breach of Covenant of Good Faith and Fair Dealing
On behalf of Plaintiff, the Class, and the New Jersey Subclass

80. Plaintiff realleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 59.

81. As described above, when Plaintiff and the Class Members provided their Personally Identifiable Information to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiff's and Class Members' Personally Identifiable Information and to timely detect and notify them in the event of a data breach.

82. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their Personally Identifiable Information in exchange for products and services provided by Defendants, as well as an implied covenant by Defendant to protect Plaintiff's and Class Members' Personally Identifiable Information in its possession.

83. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their Personally Identifiable Information to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' Personally Identifiable Information if it did not intend to provide Plaintiff and Class Members with the products and services it was offering.

84. Implied in these exchanges was a promise by Defendant to ensure that the

Personally Identifiable Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon products and services.

85. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their Personally Identifiable Information in exchange for Samsung's implied agreement to keep it safe and secure.

86. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

87. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' Personally Identifiable Information; storing the Personally Identifiable Information of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their Personally Identifiable Information to it that Defendant's data security systems failed to meet applicable legal and industry standards.

88. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

89. Likewise, all conditions required for Defendant's performance were met.

90. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

91. Plaintiff and Class Members have been or will be harmed by Defendant's breach

of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personally Identifiable Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

92. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

93. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

FOURTH CLAIM FOR RELIEF
Misrepresentation
On behalf of Plaintiff, the Class, and the New Jersey Subclass

94. Plaintiff realleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 59.

95. Defendant falsely represented to Plaintiff and Class Members that it would take appropriate and reasonable measures to safeguard their Personally Identifiable Information.

96. Plaintiff and Class members reasonably relied upon said representations in that they provided Defendant their Personally Identifiable Information.

97. Defendant's misrepresentations were material, as Plaintiff and Class Members would not have chosen to provide their Personally Identifiable Information to Samsung had they known that the information would be at heightened risk of compromise due to Samsung's lax data security.

98. As a result of Defendant's misrepresentations, Plaintiff and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses

related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

FIFTH CLAIM FOR RELIEF
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, et seq.
Plaintiff, on behalf of the Class

99. Plaintiff realleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 59.

100. Plaintiff and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

101. The Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

102. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

103. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of the State of New Jersey.

104. Defendant solicited Plaintiff and Class Members to do business and uniformly and knowingly misrepresented that by joining, their Personally Identifiable Information was safe, confidential, and protected from intrusion, hacking, or theft.

105. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Personally Identifiable Information, including by implementing and maintaining reasonable security measures.

106. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

107. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Personally Identifiable Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

108. Defendant failed to provide notice to Plaintiff and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

109. Defendant's acts and omissions, as set forth herein, evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

110. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members are required to expend sums to protect and recover their Personally Identifiable Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

111. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

SIXTH CLAIM FOR RELIEF
Declaratory and Injunctive Relief
Plaintiff, on behalf of the Class

112. Plaintiff realleges and incorporates by reference all preceding paragraphs as found in paragraphs 1 through 59.

113. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

114. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personally Identifiable Information it collected from Plaintiff and Class Members.

115. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure their Personally Identifiable Information.

116. Defendant still possesses Plaintiff's and Class Members' Personally Identifiable Information.

117. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

118. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Personally Identifiable Information in Defendant's possession is even more vulnerable to cyberattack.

119. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Personally Identifiable Information and Defendant's failure to address the security failings that led to such exposure.

120. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

121. Plaintiff, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third- party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and

contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their Personally Identifiable Information to third parties, as well as the steps they must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and violations of the consumer protection laws of New Jersey;

C. A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

2. Ordering that Defendant engage third-party security auditors and internal

personnel to run automated security monitoring;

3. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

4. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

5. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendant conduct regular database scanning and securing checks; and

7. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

LITE DEPALMA GREENBERG & AFANADOR, LLC

DATED: September 29, 2022

/s/ Joseph J. DePalma

Joseph J. DePalma
Catherine B. Derenze
570 Broad St., Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

HAUSFELD LLP
James Pizzirusso*
888 16th St., Ste 300
Washington, DC 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com

HAUSFELD LLP
Steven Nathan*
33 Whitehall Street
14th Floor
New York, NY 10004
Telephone: (646) 357-1100
snathan@hausfeld.com

DICELLO LEVITT LLC
Amy Keller*
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900
akeller@dicellolevitt.com

Counsel for Plaintiff and the Putative Class and Subclass

**To be admitted pro hac vice*

CERTIFICATION PURSUANT TO LOCAL CIVIL RULE 11.2

Pursuant to Local Civil Rule 11.2, I hereby certify that the matter in controversy is related to the following civil actions:

- *Harmer v. Samsung Electronics America, Inc.*, Civil Action No. 2:22-cv-01437 (D. Nev.), filed September 6, 2022;
- *Seirafi, et. al v. Samsung Electronics America, Inc.*, Civil Action No. 4:22-cv-01576 (N.D. Cal.), filed September 10, 2022;
- *Mark v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-07974 (S.D.N.Y.), filed September 19, 2022;
- *Becker v. Samsung Electronics America, Inc.*, Civil Action No. 3:22-cv-5723 (D.N.J.), filed September 26, 2022;
- *Dipaola et al v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-5724 (D.N.J.), filed September 26, 2022;
- *Mark v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-07974 (S.D.N.Y.), filed September 19, 2022;
- *Robinson v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-5722 (D.N.J.), filed September 26, 2022; and
- *Fernandez v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-5745 (D.N.J.), filed September 27, 2022;

I hereby certify that the following statements made by me are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment.

LITE DEPALMA GREENBERG & AFANADOR, LLC

DATED: September 29, 2022

/s/ Joseph J. DePalma

Joseph J. DePalma
Catherine B. Derenze
570 Broad St., Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

HAUSFELD LLP
James Pizzirusso*
888 16th St., Ste 300
Washington, DC 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeld.com

HAUSFELD LLP
Steven Nathan*
33 Whitehall Street
14th Floor
New York, NY 10004
Telephone: (646) 357-1100
snathan@hausfeld.com

DICELLO LEVITT LLC
Amy Keller*
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900
akeller@dicellolevitt.com

Counsel for Plaintiff and the Putative Class and Subclass

**To be admitted pro hac vice*